Vulnerability of Networks Against Critical Link Failures

Serdar Çolak
*Boğaziçi University, Dept. of Civil Engineering**

Hilmi Luş
Boğaziçi University, Dept. of Civil Engineering

Ali Rana Atılgan
Sabancı University, School of Engineering and Natural Sciences

Networks are known to be prone to link failures. In this paper we set out to investigate how networks of varying connectivity patterns respond to different link failure schemes in terms of connectivity, clustering coefficient and shortest path lengths. We then propose a measure, which we call the vulnerability of a network, for evaluating the extent of the damage these failures can cause. Accepting the disconnections of node pairs as a damage indicator, vulnerability simply represents how quickly the failure of the critical links cause the network to undergo a specified damage extent. Analyzing the vulnerabilities under varying damage specifications shows that scale free networks are relatively more vulnerable for small failures, but more efficient; whereas Erdös-Rényi networks are the least vulnerable despite lacking any clustered structure.

I. INTRODUCTION

Although the definition of network failure varies, the undisputed fact is that nodes or links can and will fail. The question of how vulnerable networks are against random failures or targeted attacks has been investigated by numerous researchers[1–3]. Whether nodes or links should be considered as subjects of these failures depends on the context: If the network under investigation is a model of the Internet[4], a computer may break down unexpectedly, which corresponds to a node failure. In the case of a transportation network[5], a highway bridge may collapse after an earthquake, in which case one rather speaks of a link failure. When power grids are the subject[6–9], power lines may fail as well as the stations whence they emanate; thus links and nodes can also fail simultaneously. Networks can also suffer from intentional attacks as opposed to random failures. Investigating the changes in the character and/or performance of networks in any of these failure scenarios is crucial to understanding the extent of damage they may suffer as well as providing insight to how they can be reinforced and determining which network types are more vulnerable.

The concept of vulnerability is associated with a system's ability to fulfill its specific purpose under imposed conditions. The purpose of the network dictates the conditions under which the system is no longer functioning, thus it must be specified in order to measure vulnerability. The primary purpose common for all networks is transmission across links. Failure scenarios generally involve a disconnection in the network, caused by a combination of link failures, such that some source nodes can no longer send signals or packages to some other target nodes. If a network is divided into several components and its connectivity is impaired, it is no longer capable of fully performing its transmission function.

A network may still function after the failure of certain nodes or links. In the instance of a highway network, if the direct route between two towns is no longer usable, the traffic may, if possible, be directed to an alternative path. If there is such a path between all pairs of nodes in the network after the failure events occur, then the network is still connected. Even if there is no such path, the traffic in the disconnected subnetworks do not have to come to a halt. Thus the network is still somewhat able to fulfill its function, although maybe not as efficiently and thoroughly as it used to. Therefore, only focusing on maintaining the overall connectivity is not always enough. Considering the case where the failures push the network to the limit where it can barely stay connected, the lack of alternative paths between node pairs inhibit network performance. Controlling the connectivity is important, but changes in network performance must also be monitored.

Network performance can be measured by various parameters which are generally based on path measures such as shortest paths, random walks, or some other measure between these two extremes. Such performance measures often deal with how efficiently signals and goods can be carried along the network. In an unrealistic model in which adding links to a network has no cost, a network designer would very likely want to connect each node to all others: In this case any transmission would be carried out by moving along only one link, and both the total number of alternative paths and the network performance attain their maximum values. Hence complete networks have the best performance and are least vulnerable, despite being rare in real life. At the other extreme, a tree network is simply connected but the failure of any single element partitions the network and

* Corresponding Author, serdar.colak@boun.edu.tr

the performance is weak. Real life networks lie in between these two examples, with varying degree distributions and more complex connectivity patterns. When geographical constraints exist, which is the case for any infrastructure network, adding certain links can be costly or even impossible.

In an attempt to quantify vulnerability in this study, path measures are used to rank the links in terms of their significance in decreasing order, and then the failure of these links are considered. Networks of equal sizes and average degrees but with different degree distributions are tested, and a formal vulnerability measure is devised based on some measured parameters. This vulnerability measure is then used along with other local and global parameters in comparing different network types. Our findings suggest that Erdös-Rényi networks are efficient, and less vulnerable but lack a local structure pattern, whereas scale free networks behave differently for varying damage specifications.

II. FAILURE SIMULATIONS

A. Centrality Measures

An important question to address when considering link failures is how to rank the links in terms of their criticality. One extreme would be to run the simulations for randomly failing links. A more systematic approach would be to rank the links according to some criteria. Over the years, network researchers introduced a number of measures for ranking the elements of a network according to their position and role in the topology. Such measures are generally termed as centrality indices[10–12]. One of these indices, the shortest path betweenness centrality, is defined to be the fraction of shortest paths between pairs of nodes in a network that pass through an element. If there is more than one shortest path between a given pair of nodes, then each such path is given equal weight with the sum of the weights equal to one. Shortest path betweenness can be thought of as a simulation in which a network with n nodes is considered and there are $n-1$ agents at each node, each with the goal of reaching each one of the remaining $n-1$ nodes using the shortest route possible. The elements that have been visited the most have the highest values.[13, 14]

Since this measure takes only the shortest paths into account, it may lead to strong biases in certain situations. Consider a network in which two clusters are connected only by two paths, one shorter than the other. All the shortest paths between nodes of the two different clusters will pass through the shorter of these paths, and the longer path will therefore have a shortest path betweenness value of zero. This longer path, however, is obviously not as insignificant for the network as this measure suggests, since once these two paths fail the network would be divided into two distinct clusters that are not connected. As an alternative, random walks can be considered instead of shortest paths. A simple random walk suggests that a walker located at a specific node chooses to move along on any one of the incident links with equal probability, and continues moving until it finds itself at the target. Walks with varying properties can be generated by manipulating the transition probabilities[15]. The random walk betweenness of a link is then defined as the number of times a random walk between node pairs passes through that link, averaged over all node pairs [16, 17].

Another measure of the importance of a link to a network is the so called average degree of a link, which is be calculated as the average degree of the two nodes at the two ends of a link. Although this measure is very blunt at distinguishing links connecting low-degree nodes to high-degree nodes from those links that connect two relatively average degree nodes, it can still be considered useful because it is a very simple mechanism and far more easy to calculate than the betweenness methods.

B. Network Simulations

Four types of networks with a fixed size (number of nodes $n = 256$) and average degree (average number of links per node $\bar{k} = 8$) are investigated via simulations: Erdös-Rényi networks, scale free networks, small world networks, and ring substrates. The former two are created by first drawing a degree sequence from the characteristic degree distribution: poisson distribution for Erdös-Rényi and power law distribution for the scale free networks [18] (Obtaining this sequence is known to be an issue for scale free networks[19]). The process is completed by randomly connecting nodes until the prescribed degree sequence is reached [20, 21]. Small world networks are produced using the Watts–Strogatz model, with a rewiring probability that corresponds to a high clustering coefficient and low shortest path length for this specific network size and average degree[22–24]. Once a network is formed, its links are ranked according to shortest path betweenness, random walk betweenness, average degree, and randomly. The highest ranked link is then broken to start the simulation of a series of failures, and this process is repeated until all links have failed.

The network reconfigures as failures occur: The degree distribution, the paths, the betweenness values all change, and therefore the link ranking also changes, sometimes drastically. Therefore recalculating the link ranking after every failure is very crucial in the sense of what the simulation physically represents. As an example, consider a highway network for which failure of a path is said to occur if the average speed on it falls below a certain limit. Once this path fails, drivers may choose move to an alternative path until this new one becomes jammed too - and so the process evolves. Although computationally cumbersome, the recalculation procedure is significant in order to properly represent the effects of failures.

Depending on the chosen ranking method, the failure ratio and the type of the network, the response in the network parameters vary. In particular, five different parameters are monitored after each link failure:

1. *Ratio of Failed Links:* The simulations move forward along a generated network by failing links one at a time until the network becomes empty. Therefore the independent variable in these simulations is the number of failed links. For easier tractability, this number is divided by the initial number of links in the network to obtain the *ratio of failed links*.

2. *Fragmentation Ratio:* A simply connected network consists of nodes where any node can reach any other. When disconnections occur and the network partitions into components, the probability of reaching a target node in one component becomes zero for the nodes in another component. Therefore the number of disconnected components becomes a reflective measure of how damaged or non-functional the network has become. This number is normalized by the total number of nodes to be fixed in the unit interval and called the *fragmentation ratio*. This parameter has been used in community detection problems as well [25]. The sizes of the components is also pertinent, and this issue has been been thoroughly investigated [26].

3. *Ratio of Disconnected Node Pairs:* The disconnection of a network of $n = 100$ into two components of 1 and 99 nodes or two components of 50 nodes each should not be considered identical failures only because the number of disconnected components are equal. Counting the number of node pairs that are disconnected provides a simple way to quantify this measure. This number can be normalized by the total number of node pairs to obtain the parameter we call the *ratio of disconnected node pairs*. Let n_i denote the number of nodes in component i. Then,

$$\begin{matrix}\textit{ratio of}\\ \textit{disconnected}\\ \textit{node pairs}\end{matrix} = \frac{\sum_{i\neq j} n_i n_j}{n\left(n-1\right)/2} \tag{1}$$

4. *Clustering Coefficient:* The ratio of the number of links between the neighbors of a node to the number of links between these neighbors if they were to form a complete graph between them is called the *clustering coefficient*[27]. It is a measure of how locally redundant a network is, since a node with a high clustering coefficient has a high number of links connecting its neighbors, and the number of alternating paths emanating from that node are also plenty. Therefore this measure can also be interpreted as an indicator of the abundance of alternative paths in the network.

5. *Efficiency:* The sum of the inverses of the lengths of the shortest paths between node pairs is the *efficiency* of a network, a parameter in the unit interval representing how short the shortest paths are[28]. In mathematical form,

$$\textit{efficiency} = \sum_{i>j} \frac{1}{l_{ij}} \tag{2}$$

where l_{ij} denotes the length of the shortest path between nodes i and j.

III. SIMULATION RESULTS

The connectivity patterns of different network types are observed to effect the simulation results, so we start this section by a brief review of the network types considered. Ring substrates are ordered networks with a degree distribution having zero variance. At the other extreme, scale free networks have betweenness distributions that obey the *power law*. The average nearest neighbor degree of scale free networks generally decrease as the node degree increases, but the average nearest neighbor clustering coefficient increases, as in Figure 4 [29]. This observation is not a contradiction and it in fact highlights the main connectivity pattern in a scale free network: few hubs with low clustering coefficient values are connected to many low-degree nodes that have higher clustering coefficients. Erdös-Rényi networks lie somewhere between these two extremes, however their totally random creation process inhibits clustering, unlike the scale free networks where there are certain zones with high clustering. Small world networks, formed by the random rewiring of a few links of a ring substrate, are known to bear the relatively high clustering of ring substrates, as well as the small shortest lengths of Erdös-Rényi networks. In this sense small world networks are an optimized version of ring substrates [30–35].

The response of ring substrates to failures is shown in Figure 1. The links that connect points which are farther apart have higher betweenness values in these networks since they act as shortcuts. When these long-range links fail, the extra stress in the weakened zone is shared by the nearby elements. In other words, the paths crossing that portion of the ring now have fewer alternatives, and therefore the links that carry this extra traffic end up having higher betweenness values. This damaged portion becomes the next failure zone until the connection is no longer there, and the ring becomes an arc. The fragmentation is almost linear for this failure scheme, but the real damage can be seen in the ratio of disconnected node pairs: before 20 percent of links fail, almost 95 percent of node pairs are already disconnected. The random and average degree failures are not extremely harmful in comparison, but networks undergo a change reminding a phase transition around when 60 to 80 percent of links have failed for these schemes.

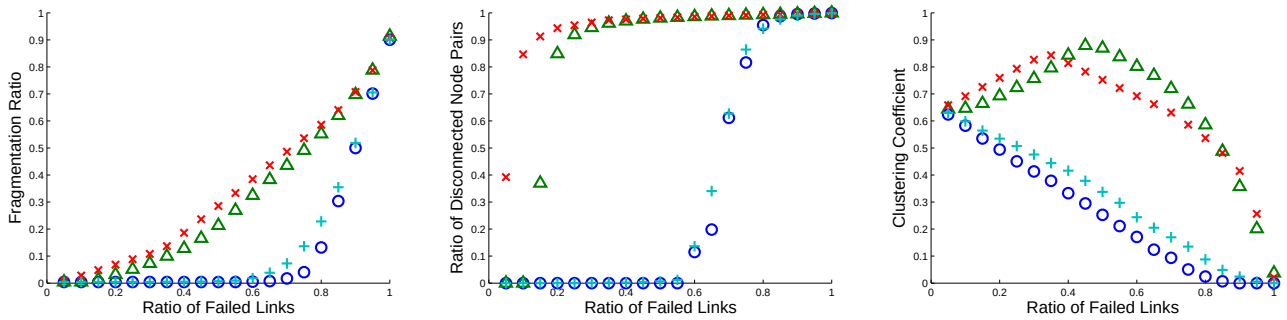

FIG. 1: The response of ring substrates of $n = 256$ and $\bar{k} = 8$, as the ratio of failed links is increased. Failure of the links with high betweenness values quickly disconnects the network into large components, each with relatively larger clustering coefficients. This process actually increases the clustering coefficient of the ring network, because the links with high betweenness values are also those that lie in regions of nodes with lower clustering coefficients, as can be seen in the third graph. The rapid increase in the ratio of disconnected node pairs happens simultaneously with the increase in the average clustering coefficient. (X : random walk betweenness, Δ : shortest path betweenness, O : average degree , + : random)

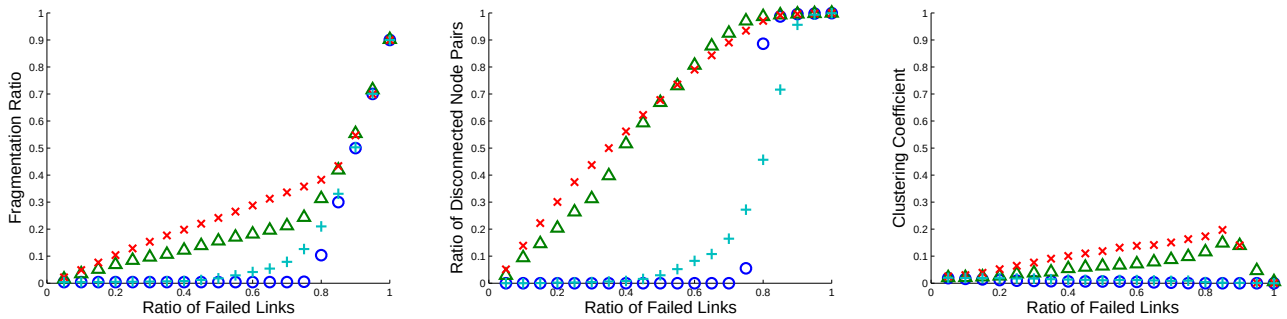

FIG. 2: The response of Erdös-Rényi networks of $n = 256$ and $\bar{k} = 8$, as the ratio of failed links is increased. In terms of fragmentation, ranking methods fail to differ by a good margin. The fragmentation is almost bilinear with a slower initial trend. Node-pair disconnection speed is very slow when compared to ring substrates. The increase in the clustering coefficient is again apparent for betweenness schemes. (X : random walk betweenness, Δ : shortest path betweenness, O : average degree , + : random)

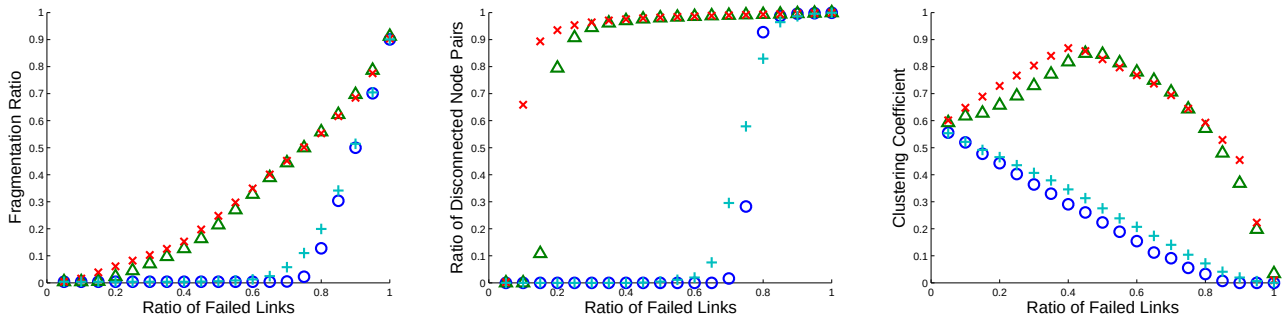

FIG. 3: The response of small world networks of $n = 256$ and $\bar{k} = 8$ with rewiring probability $\beta = 0.035$ [22], as the ratio of failed links is increased. The results are almost identical to that of the ring substrate. (X : random walk betweenness, Δ : shortest path betweenness, O : average degree , + : random)

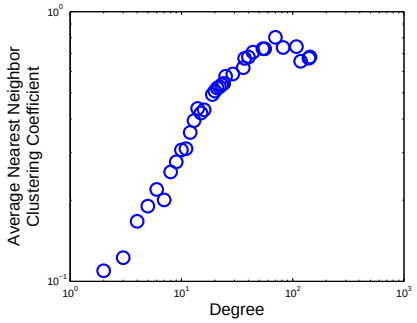

FIG. 4: The average nearest neighbor clustering coefficient as a function of the node degree for a typical scale free network with of $n = 256$ and $\bar{k} = 8$. The few high degree nodes have higher clustering coefficients compared to the low degree nodes.

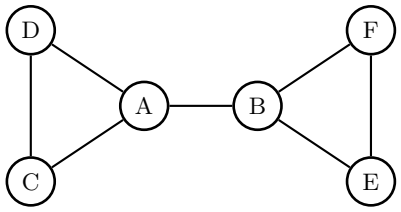

FIG. 5: A small graph illustrating the bad neighbor concept. In this configuration, all nodes have clustering coefficients equal to 1 except for A and B which have values equal to 1/3. Correspondingly, the link connecting A and B has the highest betweenness value. The failure of this link increases the clustering coefficients of these two nodes to 1 and keeps the others unchanged while at the same time disconnecting the network. Thus the clustering coefficient of the network increases, along with the fragmentation ratio and the ratio of disconnected node pairs. Nodes A and B are *bad neighbors* of each other.

The increase in the clustering coefficient observed for high betweenness failures in Figures 1 to Figure 3 may seem surprising in two aspects. The curves all peak around a ratio of failed links of 0.5, but this is only a result of the chosen network size and average degree. The more important point is that the clustering coefficient is increasing, which is counterintuitive but can simply be explained by the definition of this parameter. If the number of neighbors of a node decreases, there is a chance of an increase in the clustering coefficient of that node. The process is depicted in Figure 5. The failure of the link between these nodes disconnects the network, but increases the clustering coefficient of these networks to unity. In this case node A is said to be a *bad neighbor* of node B, and vice versa. One other process that indirectly contributes to the increase of the clustering coefficient is that a node with zero degree is no different than a node with degree one in terms of its clustering coefficient, hence the disconnection of this node leaves the average clustering coefficient of the network unchanged. Considering these processes in the larger scale, it may be concluded that the high betweenness valued links must somehow be those links that contribute negatively to the clustering coefficient, i.e. the bad neighbors.

This result shows that betweenness and clustering coefficient are somehow related. A low clustering coefficient signals the lack of alternative paths, and in such cases some incident links become the only available route for a node to connect with other regions. As a consequence, these links lying in zones with low clustering coefficients have high betweenness values and generally contribute to the bad neighbor effect: They inhibit clustering but are also good transmitters. Therefore it is reasonable to expect an increase in the overall clustering coefficient when these links fail.

In Erdös-Rényi networks, the increase in the clustering coefficient for the failure of links with high betweenness values is smaller. The parameter peaks at the points where about 60 to 90 percent of all links have failed, which corresponds to a ratio of disconnected pairs very close to 1. At this point the network consists of tiny connected subgraphs that have the smallest number of bad neighbors possible, which causes the slight increase in the clustering coefficient. It should be noted that this increase can also be caused by the very low clustering values at the initial formation.

Figure 3 shows that small world networks, differing only by a small percentage of link connections from ring substrates, fail to respond very differently than their ancestors. Comparing these two networks in the smaller failure zones (for example only up to the rewiring probability) rather than in the whole unit interval might be more appropriate. However the parameters used to measure the network response are not sensitive enough for small failures, thus making this comparison is not rewarding.

Scale free networks seem to be most prone to fragmentation, as can be observed in Figure 6. Interestingly, they do not demonstrate the increase in the clustering coefficient like other networks. On the contrary, random and average degree schemes exhibit a very fast initial decrease. This different behaviour exhibited by scale free networks is caused by the exceptional betweenness distribution of these networks: Few critical links have exceptionally high betweenness values, and many have low betweenness values. As those few critical links fail (the 0 to 10 percent of failed links zone), the clustering coefficient seems to be non-decreasing for betweenness schemes. At the end of these failures, both the fragmentation ratio and the ratio of disconnected node pairs are very high, which suggests that the network then consists of several disconnected components with similar sizes (note how low variance of component sizes result in higher ratio of disconnected node pairs). The variance of the betweenness distribution quickly decreases such that the remaining formation does not allow any link to stand out as a high betweenness element. Failure of links with high be-

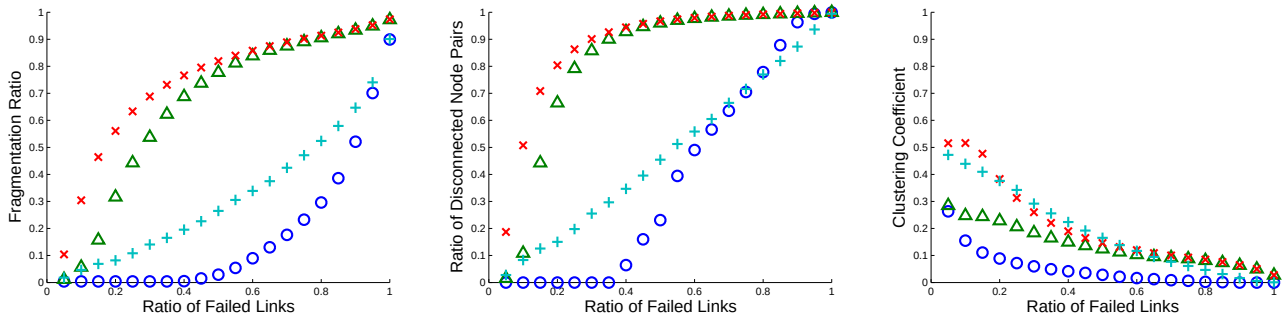

FIG. 6: The response of scale free networks of $n = 256$ and $\bar{k} = 8$, as the ratio of failed links is increased. The fragmentation is almost bilinear, but with a very steep initial trend, and node pair disconnections quickly saturate. There is no increase in the clustering coefficient. (X : random walk betweenness, Δ : shortest path betweenness, O : average degree , + : random)

tweenness values increase the clustering coefficient; conversely, failure of low betweenness valued links tend to decrease the clustering coefficient. So once a scale free network has lost its few high betweenness links, the bad neighbor effect is no longer pertinent.

It can be observed in all cases that betweenness methods are far more effective in breaking down a network when compared to the average degree and random failure schemes. The random walk betweenness is generally more dangerous than the shortest path betweenness, as observed in Figures 1 to 6. However the time required to compute the random walk betweenness repeatedly for large networks can be inhibiting, and the shortest path betweenness may provide a very practical estimate of random walk betweenness that is far more easy to calculate. Another observation for all network types is that the average degree failure scheme appears to be less destructive than random failures. This is actually to be expected since this scheme especially protects the low degree nodes. High average degree links are those that connect high degree nodes; these nodes have many other alternative paths, and even if a few of their incident links fail, the remaining ones may suffice to maintain performance. It therefore stands to reason that the probability of disconnection in the average degree scheme should be smaller than that for random failures.

Since efficiency is strongly correlated with the ratio of disconnected node pairs, the responses of the networks to failures in terms of efficiency seem generally in line with what one might anticipate. Figure 7 reveals the efficiency response, normalized by the efficiency value of each network at its initial state. Scale free networks undergo a rapid efficiency decrease for average degree and random failure schemes, unlike other network types. For betweenness failures, Erdös-Rényi networks respond strongly, the decrease behaves linearly unlike the exponential decrease in the other network types.

IV. VULNERABILITY

The general formalism for the reliability or the vulnerability of networks have so far been associated with primal cut sets[36–38]. In this section, we discuss the use of a different approach to quantify what may be termed to be the *vulnerability* of a network.

The results of the simulations indicate that betweenness methods are very efficient in determining the critical links in a network, and that their failures cause quick fragmentation. Therefore considering this response of a network against the failure of its most central links in order to formalize a vulnerability measure would be reasonable. It has been stated that shortest path betweenness is a good estimate for modeling the most detrimental link failures. Therefore here we choose to apply the shortest path betweenness as the failure regime in our calculations of vulnerability. In this context, we define the vulnerability of a network as a measure of the average speed by which the decomposition of the network causes a specified ratio of node pairs to become disconnected. One must subjectively decide on this ratio of disconnected node pairs above which the network is accepted to be performing inadequately. If this ratio, which we will call *the saturation level*, is L, then the vulnerability corresponding to this saturation level is defined as:

$$vulnerability = \frac{L}{\text{ratio of failed links at } L}. \qquad (3)$$

This definiton of vulnerability can also be interpreted as the average percent of node pairs that are disconnected per unit percentage link failures below the given saturation level, as shown in Figure 8.

Networks respond differently to varying levels of link failures, therefore it may be more informative to calculate the vulnerability of a network for a range of link failure ratios. The differences resulting from the subjective evaluation of a saturation level can also yield beneficial information. Here we use three saturation levels of 10, 50

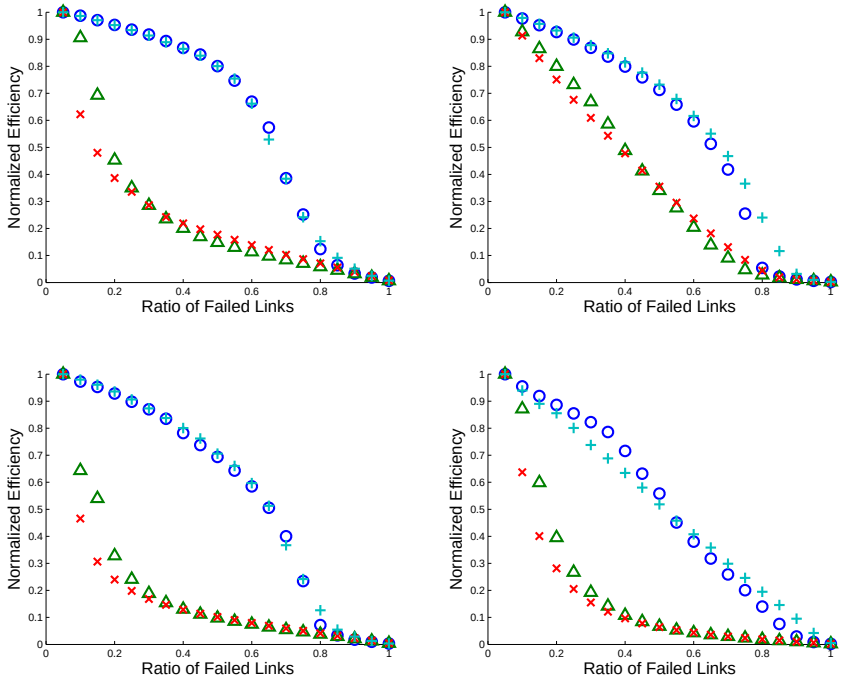

FIG. 7: The efficiency response for ring substrates (upper left), Erdös-Rényi (upper right), small world (lower left) and scale free networks (lower right) of $n = 256$ and $\bar{k} = 8$, respectively. (X : random walk betweenness, Δ : shortest path betweenness, O : average degree , + : random)

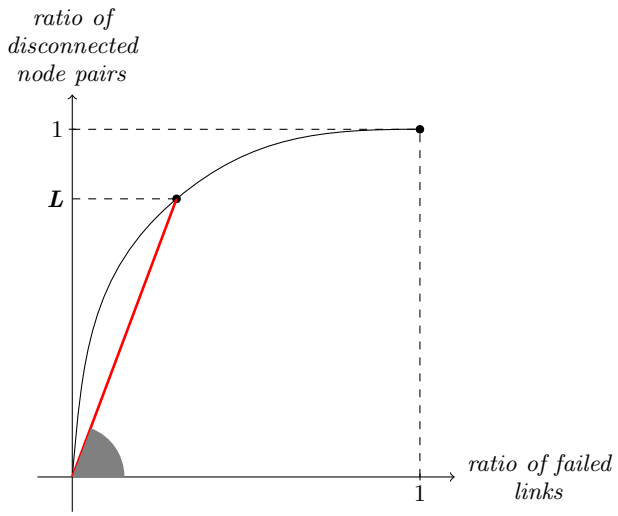

FIG. 8: A graph revealing the calculation of the vulnerability measure. The black curve depicts the change in the ratio of disconnected node pairs as the ratio of failed links increase, for the shortest path betweenness failure scheme. The red line is the linear approximation of this arbitrary curve, drawn from the origin to the black curve at the saturation level L. The slope of this red line, or the highlighted angle, is the vulnerability of the network.

and 90 percent node pair disconnections. These saturation levels represent the possible states of a network after failures occur. If the subject at hand is a highway network in which bridges are prone to collapse in case of an earthquake, the expected damage is low and short-term, which suggests choosing a lower saturation level. On the other hand if a failure is accepted to be congestion on a highway, then large, long-term, cascading failures are expected. Thus choosing a high saturation level is more appropriate. Figure 9 shows three disconnection cases that correspond to the saturation levels.

It is important to note the dependency of the vulnerability value on the selected saturation level, for slight changes in saturation levels result in different vulnerability values. Hence in order to properly decide on a saturation level, one must carefully consider the true function of the network and the failure scenarios for which the network is being tested against.

When comparing networks in these terms and bearing in mind the results obtained, it intuitively seems that improving network efficiency without increasing the average degree can only be achieved by removing short range links at the local level and adding long range links connecting formerly distant communities. However this would also cause increased vulnerability since redundancies would be removed. To utilize this information for selecting a proper network type, the initial clustering coefficient and efficiency of the network must be taken into account. One might consider vulnerability as a measure

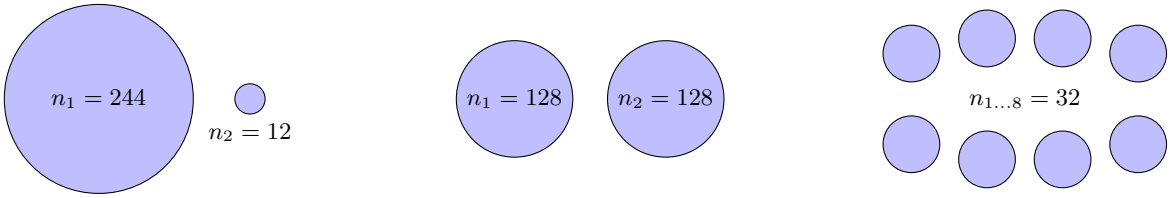

FIG. 9: Three disconnection cases for networks with $n = 256$ that approximately correspond to the three saturation levels used in this study, 0.1, 0.5 and 0.9, respectively. The disconnection of a relatively small group of nodes from the giant component depicts a saturation level of 0.1, whereas more than several components with equal sizes indicate a level of 0.9.

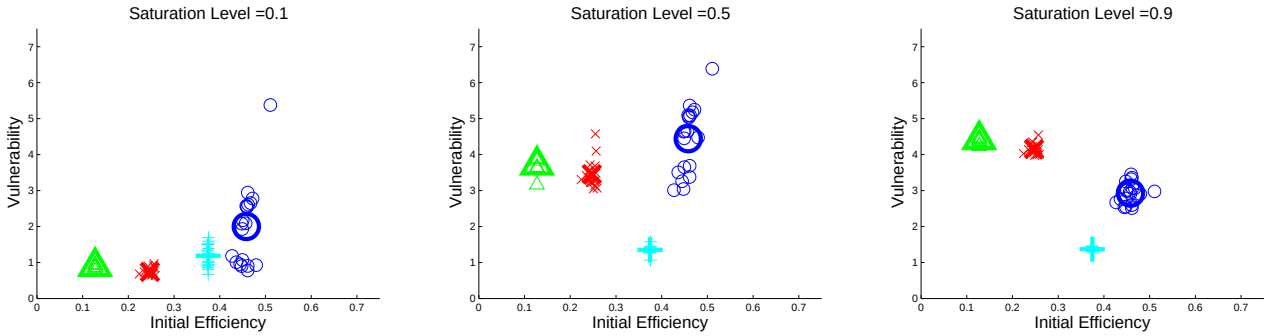

FIG. 10: Vulnerability versus initial efficiency for the four network types and saturation levels of 0.1, 0.5 and 0.9. Smaller markers depict results of a single network realization, and the bigger markers represent the mean points of such realizations. For lower saturation levels scale free networks are more vulnerable but also more efficient. Ring substrates, small world networks and Erdös-Rényi networks differ only slightly in terms of their vulnerabilities. For increased saturation levels of 0.5 and 0.9, Erdös-Rényi networks seem to be the least vulnerable and the second most efficient. Ring substrates are both vulnerable and inefficient for these levels. (X : small world networks, Δ : ring substrates, O : scale free networks, + : Erdös-Rényi networks)

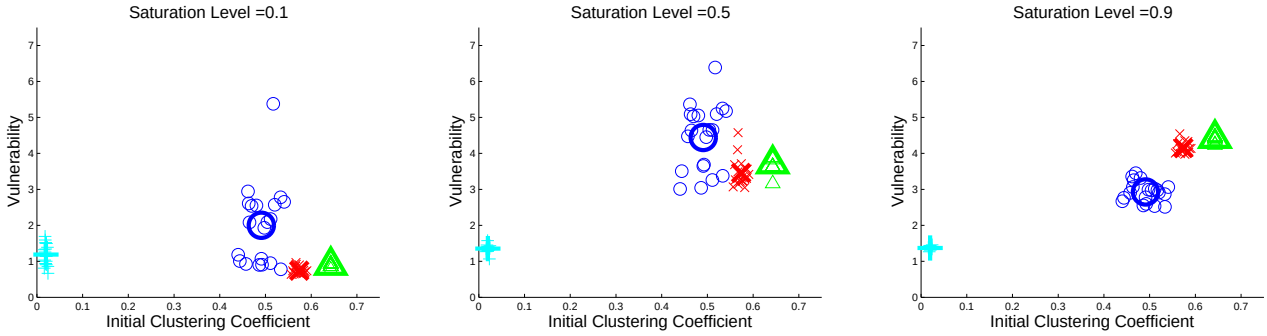

FIG. 11: Vulnerability versus initial clustering coefficient for the four network types and saturation levels of 0.1, 0.5 and 0.9. Smaller markers depict results of a single network realization, and the bigger markers represent the mean points of such realizations. Erdös-Rényi networks have very small clustering coefficients but low vulnerability as well. When compared to small world networks and ring substrates, scale free networks are less vulnerable for smaller saturation levels, but become more vulnerable with increasing saturation level. (X : small world networks, Δ : ring substrates, O : scale free networks, + : Erdös-Rényi networks)

that can be used to relate the efficiency and the clustering coefficient of a network, or simply a third dimension on which different network types can be further compared.

It can be seen from Figure 10 that scale free networks are more efficient when compared to others, but always very vulnerable for small saturation levels. For higher saturation levels, however, scale free networks are not as vulnerable as rings or small worlds. It should be noted

that Erdös-Rényi networks seem to be efficient above average and resistant to various saturation levels, therefore should be the best choice if the prime concern is to have a network that is both resistant to failures and efficient.

Figure 11 shows, on the other hand, that if a clustered network is preferred, Erdös-Rényi networks are the worst choice despite their low vulnerability values. Performances of the other network types are very similar in terms of clustering, but they differ in terms of vulnerability for different saturation levels. For the 0.1 and 0.5 levels, scale free networks are more vulnerable then the others. For the 0.9 level, however, scale free networks are less vulnerable and less clustered when compared to small world networks and ring substrates.

V. CONCLUSION

The aim of this study was to discuss how some of the well-known network types perform when they suffer link failures. To this end, various methods of ranking were used to decide on the importance of the links in the networks, and failures were carried out by removing the links starting with the highest rated one. Based on the result of the simulations, a very simple vulnerability index was defined and it was observed that this index is capable of differentiating the performance of the networks for different saturation levels.

The results obtained show that in terms of long term vulnerability, ring structures are the most vulnerable amongst the network types investigated herein, followed by small worlds. On the other hand, for relatively higher average degrees, small worlds appear to be closer to Erdös-Rényi and scale-free networks in terms of vulnerability; they are redundant on the local level despite being less efficient. In terms of short term vulnerability, however, the difference between small worlds and more random networks disappear; moreover, small worlds become less vulnerable at smaller saturation levels. Thus if the subject network is prone to failures of bigger magnitudes and if conditions permit, a power-law distribution would be a wiser choice for an infrastructure network in terms of local redundancies, vulnerability and efficiency. If, however, there is only a negligible probability of mass failures, then the vulnerability of small worlds and random networks are more or less the same; in such cases the function of the network would determine whether higher clustering is to be preferred over higher efficiency or vice versa.

[1] Réka Albert, Hawoong Jeong, and Albert Laszlo Barabasi. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, July 2000.

[2] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han. Attack vulnerability of complex networks. *Phys. Rev. E*, 65(5):056109+, May 2002.

[3] Vito Latora and Massimo Marchiori. Vulnerability and Protection of Critical Infrastructures. July 2004.

[4] Luca Dall'asta, Alain Barrat, Marc Barthelemy, and Alessandro Vespignani. Vulnerability of weighted networks. Mar 2006.

[5] B. Berche, C. von Ferber, T. Holovatch, and Y. Holovatch. Resilience of public transport networks against attacks. *The European Physical Journal B - Condensed Matter and Complex Systems*, 71(1):125–137, Sep 2009.

[6] D. Chassin and C. Posse. Evaluating North American electric grid reliability using the BarabsiAlbert network model. *Physica A: Statistical Mechanics and its Applications*, 355(2-4):667–677, Sep 2005.

[7] Ricard V. Solé, Martí Rosas-Casals, Bernat Corominas-Murtra, and Sergi Valverde. Robustness of the european power grids under intentional attack. *Phys. Rev. E*, 77(2):026102, Feb 2008.

[8] Réka Albert, István Albert, and Gary L. Nakarado. Structural vulnerability of the north american power grid. *Phys. Rev. E*, 69(2):025103, Feb 2004.

[9] Rui Carvalho, Lubos Buzna, Flavio Bono, Eugenio Gutiérrez, Wolfram Just, and David Arrowsmith. Robustness of trans-european gas networks. *Phys. Rev. E*, 80(1):016106, Jul 2009.

[10] Karen Stephenson and Marvin Zelen. Rethinking centrality: Methods and examples. *Social Networks*, 11(1):1 – 37, 1989.

[11] Stephen P. Borgatti. Centrality and network flow. *Social Networks*, 27(1):55 – 71, 2005.

[12] Stephen P. Borgatti and Martin G. Everett. A graph-theoretic perspective on centrality. *Social Networks*, 28(4):466 – 484, 2006.

[13] Linton C Freeman. A set of measures of centrality based upon betweenness. *Sociometry*, 40:35–41, 1977.

[14] M. Barthlemy. Betweenness centrality in large complex networks. *The European Physical Journal B - Condensed Matter and Complex Systems*, 38:163–168, 2004. 10.1140/epjb/e2004-00111-4.

[15] Jae Dong Noh and Heiko Rieger. Random walks on complex networks. *Phys. Rev. Lett.*, 92(11):118701, Mar 2004.

[16] M.E. J. Newman. A measure of betweenness centrality based on random walks. *Social Networks*, 27(1):39 – 54, 2005.

[17] M. E. J. Newman and M. Girvan. Finding and evaluating community structure in networks. *Phys. Rev. E*, 69(2):026113, Feb 2004.

[18] A. L. Barabasi and R. Albert. Emergence of Scaling in Random Networks. *Science*, 286(5439):509–512, October 1999.

[19] M. L. Goldstein, S. A. Morris, and G. G. Yen. Problems with fitting to the power-law distribution. *The European Physical Journal B - Condensed Matter and Complex Systems*, 41(2):255–258, September 2004.

[20] Michael Molloy and Bruce Reed. A critical point for random graphs with a given degree sequence. *Random Structures & Algorithms*, 6:161–180, 1995.

[21] R. Milo, N. Kashtan, S. Itzkovitz, M. E. J. Newman, and

U. Alon. On the uniform generation of random graphs with prescribed degree sequences. May 2004.

[22] D. J. Watts and S. H. Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):440–442, June 1998.

[23] Jon Kleinberg. The small-world phenomenon: an algorithm perspective. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, STOC '00, pages 163–170, New York, NY, USA, 2000. ACM.

[24] M. E. J. Newman. Models of the Small World: A Review. May 2000.

[25] M.C. Gonzlez, H.J. Herrmann, J. Kertsz, and T. Vicsek. Community structure and ethnic preferences in school friendship networks. *Physica A: Statistical Mechanics and its Applications*, 379(1):307 – 316, 2007.

[26] M. González, H. Herrmann, and A. Araujo. Cluster size distribution of infection in a system of mobile agents. *Physica A: Statistical Mechanics and its Applications*, 356(1):100–106, October 2005.

[27] Duncan J. Watts. *Small Worlds: The Dynamics of Networks between Order and Randomness (Princeton Studies in Complexity)*. Princeton University Press, illustrated edition edition, November 2003.

[28] L. Dueas-Osorio, J. I. Craig, and B. J. Goodno. Seismic response of critical interdependent networks. *Earthquake Engineering & Structural Dynamics*, 36(2):285–306, September 2007.

[29] S. Colak. Vulnerability of networks against rank ordered independent link failures. Master's thesis, Boğaziçi University, June 2010.

[30] S. N. Dorogovtsev and J. F. F. Mendes. Evolution of networks. *Advances in Physics*, 51(4):1079–1187, 2002.

[31] Réka Albert and Albert-László Barabási. Statistical mechanics of complex networks. *Rev. Mod. Phys.*, 74(1):47–97, Jan 2002.

[32] Guido Caldarelli and Alessandro Vespignani. *Large Scale Structure and Dynamics of Complex Networks: From Information Technology to Finance and Natural Science (Complex Systems and Interdisciplinary Science)*. World Scientific Publishing Company, June 2007.

[33] M. E. J. Newman. Assortative mixing in networks. *Phys. Rev. Lett.*, 89(20):208701, Oct 2002.

[34] M. E. J. Newman. Mixing patterns in networks. *Phys. Rev. E*, 67(2):026126, Feb 2003.

[35] Romualdo Pastor-Satorras, Alexei Vázquez, and Alessandro Vespignani. Dynamical and correlation properties of the internet. *Phys. Rev. Lett.*, 87(25):258701, Nov 2001.

[36] David R. Karger. A randomized fully polynomial time approximation scheme for the all terminal network reliability problem. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, STOC '95, pages 11–17, New York, NY, USA, 1995. ACM.

[37] Daryl D. Harms, Miro Kraetzl, Charles J. Colbourn, and John S. Devitt. *Network Reliability: Experiments with a Symbolic Algebra Environment*. CRC Press, Inc., Boca Raton, FL, USA, 1995.

[38] Michael O. Ball, Charles J. Colbourn, and J.S. Provan. Network reliability. 1992.